

REMARKS

This response is made in order to bring the application to allowance. It follows the paragraphs of the office action for ease of entering the amendments to the claims. Paragraphs from the office action are in italics and indented from the responses. A listing of the claims is provided as required in the new USPTO amendment practice per 37 CFR 1.121.

DETAILED ACTION

Claim Rejections - 35 USC § 101

Claim 23-28, 36-40 are rejected under 35 ASSOC.. 101 because claim 23 recites a method comprising: " generating a TCR commitment opening function for extracting a data string committed to by at least one TCR commitment message, utilizing a corresponding TCR opening string , and employing a TCR function and a regular commitment scheme used in generating TCR commitment message and used in generating corresponding TCR opening string". Steps of claim 23 is merely a series of function applied on various strings or messages with no concrete and tangible result.

In response, applicant respectfully states that in order to overcome the 101 rejection, claim 23 is amended to include the limitations of claims 32 and 34. Claims 32 and 34 are canceled. Thus claim 23 and claims that depend thereupon are allowable.

Dependent claims 32-34 are also rejected by virtue of their dependencies.

Apparatus claims 24-25 corresponding to method claims 23 are also rejected for the same reasons stated above.

Dependent claims 26-28, 36-40 are also rejected by virtue of their dependencies.

In response, applicant respectfully states that all these claim are allowable because of the allowance of claim 23 as amended.

DOCKET NUMBER: YOR919990229US2

-11/17-

1 ***Claim Rejections - 35 USC § 112***

2 *The following is a quotation of the second paragraph of 35 USC. 112: The specification shall conclude*
3 *with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant*
4 *regards as his invention.*

5 *Claims 26-28, 31 and 37-40 are rejected under 35 USC. 112, second paragraph, as being*
6 *indefinite for failing to particularly point out and distinctly claim the subject matter which*
7 *applicant regards as the invention.*

8 *Claim 26 recites the limitation "said regular commitment scheme" in lines 20-21. There is*
9 *insufficient antecedent basis for this limitation in the claim. Dependent claims 27-28 and 39 are*
10 *rejected by virtue of their dependencies.*

11 In response, applicant respectfully states that claim 26 is
12 amended to depend upon method claim 10, and to change 'said
13 regular commitment scheme' to 'a regular commitment scheme'. This
14 overcomes the 112 rejection and claim 26, and claims 27, 28, and
15 39 which depend thereon are allowable.

16 *Claims 26-28,37-40 are method claims depending from an apparatus claim 25 (computer*
17 *program product). Dependent method claim should not be depending from a base method claim.*

18 In response, applicant respectfully states that claim 2 as
19 amended depends on method claim 10. This overcomes the 112
20 rejection and claim 26-28, and 37-40 which depend thereon are
21 allowable.

22 *Claims 31 and 35 recite "any TCR function" and "any regular commitment". The terms "any*
23 *TCR function" and "any regular commitment" are not determinant and are relative terms which*
24 *renders the claim indefinite. The specification does not provide a standard for ascertaining the*
25 *requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the*
26 *scope of the invention.*

1 In response, applicant respectfully states that claims 31 and 35
2 are amended to include a portion of the limitation in claim 43.
3 Claim 43 is amended to delete that portion included in claim 31.,
4 and to depend on claim 31. This overcomes the 112 rejection and
5 makes claims 31 and 35 allowable.

6 *Dependent claims 41-43 are rejected by virtue of their dependencies.*

7 The amendments of claims 31 and 35 overcomes the 112 rejection
8 and claim 41-43 which depend thereon are allowable.

9 *Double Patenting*

10 *The non statutory double patenting rejection is based on a judicially created doctrine grounded*
11 *in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper*
12 *timewise extension of the "right to exclude" granted by a patent and to prevent possible*
13 *harassment by multiple assignees. See In re Goodman, 11 F.3d 1046,29 USPQ2d 2010 (Fed. Cir.*
14 *1993); In re Longi, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); In re Van Ornum, 686 F.2d*
15 *937, 214 USPQ 761 (CCPA 1982); In re Vogel, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and,*
16 *In re Thorington, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).*

17 *A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome*
18 *an actual or provisional rejection based on a nonstatutory double patenting ground provided the*
19 *conflicting application or patent is shown to be commonly owned with this application. See 37*
20 *CFR 1. 130(b).*

21 *Effective January 1, 1994, a registered attorney or agent of record may sign a terminal*
22 *disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).*

23 *Claims 1-9, 15, 17-18,20 and 21 are provisionally rejected under the judicially created doctrine*
24 *of obviousness-type double patenting as being unpatentable Over claims], 6,] 2, 13.] 4, 18,46 and 60 of*
25 *copending Application No. 09/307.493. Although the conflicting claims are not identical, they*
26 *are not patentably distinct from each other because claim 1 of the copending application '493*

DOCKET NUMBER: YOR919990229US2

-13/17-

1 *is directed to a method of generating a signature for a message employing a public/private*
2 *key pair in which the private key includes at least one enhancing key; and a public key which*
3 *includes a TCR commitment (or a regular commitment recited in claim 12 of the Application*
4 *'493) to at least one enhancing key recited in claims 1 and 3 of the pending application, see*
5 *claim 1, lines 4-6.*

6 In response, applicant respectfully states that although he takes
7 exception with the Examiner's assertion that the present
8 application suffers from, 'obviousness-type double patenting with
9 regard to '493, in order to expedite allowance of the present
10 application, a terminal disclaimer is included herewith.

11 *Claim Rejections - 35 use § 102*

12 *The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the*
13 *basis for the rejections under this section made in this Office action: A person shall be*
14 *entitled to a patent unless-(a) the invention was known or used by others in this country,*
15 *or patented or described in a printed publication in this or a foreign country, before the*
16 *invention thereof by the applicant for a patent.*

17 *Claims 10, 44 and 29 are rejected under 35 U.S.C. 102(a) as being anticipated by*
18 *M. Belare, P. Rogaway, Collision-Resistant Hashing: Towards making UOWHFs*
19 *Practical, Department of Computer Science & Engineering, University of California at*
20 *San Diego, July 1997. Belare teaches a signing with an TCR Hash family where the*
21 *signing algorithm chooses K (i.e. a commitment) anew for each message (i.e. a first*
22 *string). Belare further teaches that the key K is included with the signature. That is a*
23 *second TCR function is applied to a second string that includes the commitment (i.e. key*
24 *K), see pages 26-27, see also page 28. Belare discloses the steps of verifying a message*
25 *using TCR function (i.e. a TCR de-commitment function) for verifying the TCR*
26 *commitment message generated, see page 26.*

27 *Claim 44 is an apparatus corresponding to method claim 29. It is rejected for the same*
28 *reasons stated in the statement of rejection of claim 29 above.*

29 In response, applicant respectfully states that the following
30 traverses the rejection of claims 10, 29 and 44 pursuant to 35
31 USC 102(a) as being anticipated by M. Bellare, P. Rogaway,
32 Collision-Resistant Hashing: Towards making UOWHFs Practical,
33 1997, specifically pages 26, 27 and 28.

1 Whereas, the present invention is clearly based on the use of
2 UOWFH's (or TCR functions) in a manner that is described in
3 Bellare et. al., the above reference, the above reference and
4 claims 10,29,44, are in regard to two entirely different
5 cryptographic primitives. The reference deals with use of TCR
6 functions for creating digital signatures while the present
7 invention uses TCR functions for creating an entirely new and
8 different cryptographic primitive called a TCR-commitment, as in
9 claims 10, 29 and 44.

10 Digital Signatures and commitments (or TCR-commitments) are two
11 very different cryptographic primitives. In a digital signature,
12 the message that is signed is public knowledge and there is NO
13 requirement that a signature hide all information about the value
14 that is signed. In contrast a commitment or TCR-commitment by
15 definition has to hide all information about the value that is
16 committed (see Page 22 of application).

17 Bellare and Rogaway in pages 26, 27 and 28 are saying that for a
18 message M (which may be public, or even chosen adversarially),

19 $K, \text{Sign}(K || H_K(M))$

20 represents a signature for message M , where K is a randomly
21 chosen key K, H_K is a keyed TCR function and Sign is any digital
22 signature function. Note that there is no requirement that
23 $\text{Sign}_K(K || H_K(M))$ hide all information about M because M is
24 expected to be public and even if it is not, for most signature
25 schemes such as RSA, given the string $\text{Sign}(K || H_K(M))$ one can
26 easily derive K and $H_K(M)$ which easily constitutes information
27 about M. For instance given only K and $H_K(M)$ one can still
28 determine that the unknown M is not the same as a known M'
29 simply by computing $H_K(M')$ and noting that it is different from

DOCKET NUMBER: YOR919990229US2

-15/17-

1 H_K(M). This constitutes leakage of information about M. In a
2 more concrete example that makes this leakage clear, assume that
3 M is a sealed bid for a contract then the Bellare-Rogaway
4 signature, $K, \text{Sign}(K || H_K(M))$ will not be suitable since if
5 there were a small number (say n) of possibilities $M_1, M_2, \dots,$
6 M_n for the bid, anyone knowing $K, \text{Sign}(K || H_K(M))$ can
7 exhaustively test them all n of them and determine the actual
8 bid.

9 In contrast the present invention is creating a TCR commitment
10 using a regular commitment. Here we are using $\text{Sign}(K ||$
11 $H_K(\text{Commit}(M)))$ as a TCR commitment for value of M . Note that
12 knowing K and $H_K(\text{Commit}(M))$ gives no information about M since
13 even knowing $\text{Commit}(M)$ gives no information about M by the
14 definition of a commitment function. Thus claims 10, 29 and 44
15 and all claims that depend thereupon are allowable over the cited
16 art.

17 *Allowable Subject Matter*

18 *Claims 11-14, 16, 19, 22 and 30 are objected to as being dependent upon a rejected base*
19 *claim, but would be allowable if rewritten in independent form including all of the*
20 *limitations of the base claim and any intervening claims.*

21 The amendments to the claims presented and described above
22 overcome the rejections of the claims, and the objected-to claims
23 11-14, 16, 19, 22 and 30, which depend thereupon are allowable.
24 Thus Claims 11-14, 16, 19, 22 and 30 are allowable.

25 It is anticipated that this amendment brings the application to
26 allowance, and favorable action is respectfully solicited. In
27 the unlikely event that any claim remains rejected, please
28 contact the undersigned by phone in order to discuss the
29 application.

DOCKET NUMBER: YOR919990229US2

-16/17-

1 Please charge any fee necessary to enter this paper to deposit
2 account 09-0468.

3 Respectfully submitted,

4 By: Louis Herzberg
5 Dr. Louis P. Herzberg
6 Reg. No. 41,500
7 Voice Tel. (914) 945-2885
8 Fax. (914) 945-3281

9 IBM CORPORATION
10 Intellectual Property Law Dept.
11 P.O. Box 218
12 Yorktown Heights, New York 10598

DOCKET NUMBER: YOR919990229US2

-17/17-